

Innominate mGuard

Version 4.2.3 - Release Notes

Innominate Security Technologies AG
Albert-Einstein-Straße 14
12489 Berlin, Germany
Tel.: +49 30 6392-3300
e-mail: contact@innominate.com
<http://www.innominate.com/>

© Innominate Security Technologies AG

October 2007

“Innominate” and “mGuard” are registered trademarks of the Innominate Security Technologies AG. All other brand names or product names are trade names, service marks, trademarks, or registered trade marks of their respective owners.

mGuard technology is protected by the German patents #10138865 and #10305413.

Further national and international patent applications are pending.

No part of this documentation may be reproduced or transmitted in any form, by any means without prior written permission of the publisher.

All information contained in this documentation is subject to change without previous notice. Innominate offers no warranty for these documents. This also applies without limitation for the implicit assurance of scalability and suitability for specific purposes.

In addition, Innominate is neither liable for errors in this documentation nor for damage, accidental or otherwise, caused in connection with delivery, output or use of these documents.

This documentation may not be photocopied, duplicated or translated into another language, either in part or in whole, without the previous written permission of Innominate Security Technologies AG.

Innominate Document Number: RN204232807-004

1 Features of this Release

This section documents the features provided by this release.

1.1 Product Description

1.1.1 Supported Hardware

mGuard Smart/Core

- Ultra Compact Single Board Computer
- Intel IXP42x 533 or 266 MHz network processor
- One serial RS232 interface [mGuard Core only]
- 32MB or 64MB SDRAM
- 16MB FLASH
- Power supply via USB port (5V 500mA DC) or external (110 - 230 V AC)
- Operating temperature 0-70 °C (mGuard Core only) 0-40 °C (mGuard Professional, Enterprise)
- Relative humidity: 20-90%, non condensing
- Two Ethernet interfaces 10/100 Mbit/s
- RJ45 plug, short wire with RJ 45 plug (mGuard Professional, Enterprise)
- RJ45 plug, JST KR plug male (mGuard Core only)
- Three indicator LEDs
- Rescue button
- External power supply, USB power supply

mGuard Delta

- Compact Single Board Computer
- Intel IXP42x 533 or 266 MHz network processor
- One serial RS232 interface
- 64MB or 128MB SDRAM
- 16MB or 32MB FLASH
- Power supply via external adapter (110 - 230 V AC)
- Operating temperature 0-40 °C
- Relative humidity: 20-90%, non condensing
- One Ethernet interface 10/100 Mbit/s, RJ45 plug
- One integrated 4 port Ethernet switch 10/100 Mbit/s, RJ45 plug
- One indicator LED
- Rescue button

mGuard PCI

- 32bit low profile PCI 3.3V/5V universal card, 66MHz capable
- Intel IXP42x 533 or 266MHz network processor
- One serial RS232 interface
- 32MB or 64MB SDRAM
- 16MB Flash

- PCI bus operation with driver or PoPCI (Power over PCI) mode
- Operating temperature 0-70 °C
- Two Ethernet interfaces 10/100Mbit/s, RJ45 plug
- Four indicator LEDs
- Rescue button

mGuard Blade

- mGuard blade ID-Bus system
- Intel IXP42x 533 or 266MHz network processor
- One serial RS232 interface
- 64MB SDRAM
- 16MB Flash
- Operating temperature 0-40 °C
- Two Ethernet interfaces 10/100Mbit/s, RJ45 plug
- Four indicator LEDs
- Rescue button

EAGLE mGuard/mGuard Industrial

- Rail mountable case
- 24V industrial power supply standard
- Intel IXP42x 533MHz network processor
- One serial V.24 interface
- 64MB SDRAM
- 16MB Flash
- Operating temperature 0-55 °C
- Two Ethernet interfaces 10/100Mbit/s, RJ45 plug
- Seven indicator LEDs
- Rescue button

1.1.2 Software

VPN Functionality

- Authentication by Pre-Shared Secret Key
- Authentication by X.509 v3 Certificate
- Multi point VPN
- IPsec DES Encryption 56 bit
- IPsec Triple DES Encryption 168 bit
- IPsec AES Encryption 128bit, 192bit, 256bit
- Hardware encryption support [AES support depending on processor stepping]
- Tunnel and Transport Mode IPsec
- RSA (up to 4096 bit key)
- MD5 128 bit, SHA-1 160 bit check sum
- Main and Quick Procedure for Internet Key Exchange (IKE)
- Perfect Forward Secrecy (PFS)
- NAT-T Support
- Dead Peer Detection (DPD) per RFC3709

- 1:1 Address Rewriting in Tunnel (local and / or remote network)
- Automatic ARP responses for remote net if it is (rewritten to) a subnet of a local net (router mode)
- L2TP (Layer 2 Tunneling Protocol) Support (license controlled)

Firewall

- Configurable firewall rules for incoming and outgoing traffic with optional logging
- Configurable firewall rules for incoming and outgoing traffic in VPN tunnels with optional logging
- Logging with unique identification of firewall rules
- Stateful Inspection
- Anti Spoofing
- SYN and ICMP flooding protection
- L2 MAC/Protocol based filtering support (stealth mode)
- Firewall with user authentication feature
- Firewall Redundancy (license controlled)

Networking

- Stealth Modes: single client automatic, single client static, multi-client
- Router Mode
- PPPoE Mode
- PPTP Mode
- NAT and Port Forwarding
- Static Routing Tables
- Multiple IP addresses on Interfaces
- VLAN support (VLAN tags) in router and stealth mode
- L2 Redundancy (port monitoring) in stealth mode

Other Functions

- Automatic Software Update
- Browser Administration
- SNMP Agent v1/2 and v3
- SNMP Traps v1
- SSH Administration via Command Line
- Remote Syslog Server Support
- Configuration Profile Handling
- Transparent Bridging
- NTP Support
- DHCP Server and DHCP Relay Agent
- Dynamic DNS Registration
- LLDP Link Layer Discovery Protocol
- Blade: automatic configuration handling by blade controller
- EAGLE mGuard/mGuard Industrial: ACA Auto Configuration Adapter support
- Copy Protected File System
- Hardware Integrity Check
- Software Integrity Check

- Plug and Play Configuration
- Virus protection (optional), see issue “Anti-Virus: operation on hardware with 32MB RAM”

1.2 Changes Since Previous Releases

1.2.1 Changes made between 4.2.2 and 4.2.3

- Fixed race condition with Dead Peer Detection (DPD) which made VPN tunnels unusable if DPD was attempted during the re-negotiation of the IPsec SA
- Added support for automatic licence installation via Innominate's Device Manager release 1.2

1.2.2 Changes made between 4.2.1 and 4.2.2

- Fixed security issues with ClamAV: CVE-2007-0897, CVE-2007-0898, CVE-2007-0899, CVE-2007-1745 and CVE-2007-2650
- Fixed Dead Peer Detection (DPD) for multiple connections between same sites
- Fixed irritating log message for VPN regarding “/proc/net/ipsec_eroute”
- Fixed Local Update to version 5.0.0 and later for devices with 32 MB RAM

1.2.3 Changes made between 4.2.0 and 4.2.1

- Fixed ARP replies for the firewall redundancy feature
- Fixed configuration pull in stealth mode with boot time schedule
- Fixed “restart” button in GUI for VPN tunnels
- Fixed security issue with ClamAV: mails exceeding max. MIME nesting level are considered as infected now; see CVE-2006-6481
- Fixed SNMP traps sent upon power supply outage: correct power supply instance is referenced now

1.2.4 Changes made between 4.1.1 and 4.2.0

- Extended support for Innominate Device Manager 1.1
- Extended 1:1 NAT within VPN tunnels to optionally translate remote network addresses
- Added automatic ARP responses for remote networks of VPN connections in router mode if they are (translated to) a subnet of a local network
- Improved Dead Peer Detection (DPD) regarding NAT-T
- Added new target for semi-automatic online updates: minor releases
- Fixed security issues with ClamAV: CVE-2006-4182, CVE-2006-5295 and CVE-2006-5874
- Fixed dynamic timeout option of the user firewall
- Improved blocking of VPN traffic during reconfiguration (please see issue “Traffic bypasses VPN during reconfiguration” below)
- Fixed fully automatic updates initiated by Innominate Security Configuration Manager (ISCM)

1.2.5 Changes made between 4.1.0 and 4.1.1

- Fixed firewall rule log identifiers for 11th and following VPN connection or user firewall template
- Fixed VPN logging not to include the machine's private key
- Fixed file handling with ACA 21 on EAGLE mGuard platform

1.2.6 Changes made between 4.0.4 and 4.1.0

- Added support for EAGLE mGuard platform
- Added support for Innominate Device Manager 1.0
- Added support for higher compression of AV databases
- Added support for RADIUS group authentication for user firewall
- Added SNMP traps for user firewall
- Added dynamic timeout option and administrator logout feature for user firewall
- Added firewall line information to logs and provide new unique ID
- Added lookup mechanism to resolve log information to firewall ruleset
- Added „restart“ option to Dead Peer Detection in VPN
- Added L2/Ring Coupling redundancy support
- Apply (outgoing) firewall rules to virus scanned traffic as well (optionally)
- Modified login screen to separate administrative login from user firewall operation
- Reduced timeout settings for online software update
- Fixed race in ICMP flood protection/connection tracking that could lead to a higher packet rate than configured.

1.2.7 Changes made between 4.0.3 and 4.0.4

- Fixed security issue with ClamAV: <http://www.clamav.net/security/0.88.4.html>
It allowed a Denial of Service attack on the AntiVirus function.

1.2.8 Changes made between 4.0.2 and 4.0.3

- Fixed problem with IPsec and firewall failure only occurring after a fresh installation of the 4.0.2 firmware image (jffs2.img.p7s) using the flash procedure.

1.2.9 Changes made between 4.0.1 and 4.0.2

- Fixed accidental removal of VPN configurations during software update if the number of configured connections is near to the licensed maximum count
- Fixed possible failure on re-registration at DynIP service after PPPoE reconnect during software update
- Fixed problem with VPN tunnels not being established between software update and reboot

1.2.10 Changes made between 4.0.0 and 4.0.1

- Fixed VPN configuration page: IKE options „Yes/No“ switch inverted (GUI only, profiles or SNMP are not affected)
- Fixed memory leak in SNMP agent
- Fixed AV database download not honoring configuration changes
- Fixed AV database download not refreshing damaged database files
- Fixed AV false positives for CAB files (windows update)

- Fixed logging to correctly use timezone settings

1.2.11 Changes made between 3.1.1 and 4.0.0

- Completely revised GUI
- GUI authentication session based instead of 'HTTP Basic Authentication'
- New AV scan engine 'ClamAV'
- New firewall templates with user authentication (optionally via RADIUS)
- Added 1:1 NAT within VPN Tunnels (Router Modes)
- Added semi-automatic handling of online updates
- Added online license handling via Internet
- Removed license restrictions for MAU management, SNMP, LLDP, Remote Syslog so that these features can now be used on all devices
- Fixed failure of SNMP agent when trying to set empty strings for SysLocation.0, SysContact.0, and SysName.0
- Fixed incorrect values of ifOperStatus and ifAdminStatus if port was disabled
- Fixed possible failure in VPN startup when external IP changed often
- Fixed slow network performance with IPX protocol (Stealth Mode with explicit permission for IPX in MAC filtering required)
- Fixed handling of broadcast flag in DHCP Relay mode (affecting Cisco IP phones as clients)
- Fixed problem in AV with FTP protocol for some servers sending excessively long greeting messages.

1.2.12 Changes made between 3.1.0 and 3.1.1

- Added mGuardSysProduct MIB object allowing detailed identification of mGuard product type
- Changed some MIB objects from OCTET-STRING to DisplayString
- Fixed problem in AVP pattern update preventing update after several weeks of operation
- Fixed memory leak in SNMP server
- Fixed missing LinkUp/Down Traps on mGuard Delta ports 4-7
- Fixed crash when deleting VPN tunnel under excessive load
- Fixed incoming firewall handling in Stealth Mode inside a VPN tunnel connection using NAT-T
- Fixed blocking of ICMP from internal interface if SNMP from internal interface was explicitly forbidden

1.2.13 Changes made between 3.0.1 and 3.1.0

- Added support for mGuard Delta platform
- Added support for FTP protocol to AVP proxy
- Added support for %any in stealth mode
- Added SNMP traps to inform about redundant firewall state
- Extended LLDP to support the lldpLocalSystemData table
- Extended administrative access firewall rules to allow protection from intern
- Fixed per rule firewall logging in serial/PPP access
- Fixed problem in multi stealth firewall redundancy: switching priorities could cause excessive sending of ARP frames

- Fixed excessive sending of power fail traps on mGuard Blade
- Speed up handling of RFC1213 SNMP table with large amounts of ARP entries

1.2.14 Changes made between 3.0.0 and 3.0.1

- Fixed SSL/TLS security issue (CAN-2005-2969) affecting HTTPS access
- Fixed MGUARDDB-MIB using negative numbers in enumeration types
- Fixed NAT not working on external interface with activated VLAN
- Fixed VPN in stealth mode to not re-negotiate new keys (SA) too often
- Fixed SNMP traps for AVP updates
- Fixed user password functionality
- Fixed file descriptor leakage in AVP SNMP trap processing
- Modified LLDP page to show more information

1.2.15 Changes made between 2.3.1 and 3.0.0

- Added multiple client stealth function
- Added option to use dedicated management IP address in stealth modes
- Added firewall redundancy support in router and multiple client stealth mode
- Added Layer 2 MAC/protocol based filtering (stealth mode)
- Added support for SNMP traps
- Added VLAN support (VLAN tag) in router and stealth mode
- Added LLDP Link Layer Discovery Protocol support
- Added support for DHCP server in stealth mode
- Added extended support for mGuard blade platform (configuration deployment, status information)
- Added support for ACA Auto Configuration Adapter for mGuard Industrial platform
- Added additional configuration options for serial port
- Added configuration options for ARP timeout and MTUs
- Performance enhancements in router and stealth mode
- Reworked mGuard MIB to new MGUARDDB-MIB
- Dropped support for AVP on 32MB devices
- Use automatic IP detection mode (DynDNS.org) to also support this protocol behind NAT firewalls
- Fixed SNMP value for ipAdEntNetMask
- Fixed kernel security issue CAN-2005-2096 (zlib); notes: user space zlib on mGuard would not be affected, kernel issue probably not exploitable on mGuard

1.2.16 Changes made between 2.3.0 and 2.3.1

- Fixed L2TP tunnel problem with Windows XP/SP2
- Fixed AVP proxy operation: under certain conditions the maximum number of concurrent connections could not be used

1.2.17 Changes made between 2.2.0 and 2.3.0

- Added DHCP Relay Agent function
- Added 1:1 NAT support
- Added lease time configuration to DHCP server
- Added support for user credentials (basic authentication) for online update

- Added configuration polling support
- Added H.323 NAT/connection tracking helper module (default: disabled)
- Added AVP support for http-proxy operation (also handling „ftp-over-http“: ftp via http proxy server)
- Added more flexible IPsec/L2TP configuration
- Added japanese language WEB-configuration interface
- Added log-messages for configuration changes
- Fixed various issues with virus scanning component
- Fixed security issue CAN-2005-1263 (elf-loader); note: exploit would have required a local login on mGuard
- Fixed possible crash with IGMP traffic

1.2.18 Changes made between 2.1.6 and 2.2.0

- Added virus scanning support in Stealth Mode
- Added „Default Route through VPN“ feature
- Added broadcast IP and WINS server to DHCP server options
- Added restrictions for source IPs in port forwarding rules
- Added more information to firewall logs
- Added packet consistency check „unclean match“ (enabled by default)
- Added option to load virus signature updates through proxy server
- Modified virus signature server settings to Innominate server (see Section „Updating from previous releases“!)
- Modified Stealth Mode to no longer restrict services to only 2 servers
- Improved PPPoE throughput for high speed connections »10Mbit/s
- Fixed various issues with virus scanning component
- Fixed issue with NTP not starting correctly in router modes when using FQDN instead of IP addresses
- Fixed security issue CAN-2005-0384 (remote Linux DoS on ppp servers); Note: actual impact and exploit are not discussed in the vulnerability database
- Fixed security issue CAN-2005-0794 (potential DOS in load_elf_library()); note: exploit would have required a local login on mGuard

1.2.19 Changes made between 2.1.5 and 2.1.6

- Fixed issue with Kaspersky AVP update being performed too frequently
- Fixed security issue reported on ARM-Linux kernel mailing list (syscall() exploit); note: exploit would have required a local login on mGuard

1.2.20 Changes made between 2.1.4 and 2.1.5

- Fixed issue with new Kaspersky AVP database structure

1.2.21 Changes made between 2.1.3 and 2.1.4

- Added support for additional 64MB hardware versions
- Added MAU (Media Access Unit) management (Enterprise, Enterprise XL)
- Fixed issue with „Provider Defined“ Nameservers failing if more than one name server is listed
- Fixed issue with PSK (Preshared Secret Key) not being properly checked for control characters preventing VPN connection from being initialized

- Fixed security issue CAN-2004-1235 (uslib() exploit); note: exploit would have required a local login on mGuard
- Fixed several security issues reported with grsecurity 2.1.0 release; note: exploits would have required a local login on mGuard

1.2.22 Changes made between 2.1.2 and 2.1.3

- Added support for mGuard-PCI hardware platform
- Fixed issue with possible „gaiconfig –set-all failure“ for manually crafted settings
- Fixed issue with log messages showing wrong date (0 instead of 12 for December)
- Fixed security issue CAN-2004-1016 (scm_send local DoS); note: exploit would have required a local login on mGuard
- Fixed security issue CAN-2004-1070 (binfmt_elf exploit); note: exploit would have required a local login on mGuard
- Fixed security issue CAN-2004-1137 (igmp local/remote DoS); note: could not be exploited on mGuard anyway
- Fixed security issue with ip_options_get (no CAN-number assigned); note: exploit would have required a local login on mGuard
- Fixed security issue with vc_resize (no CAN-number assigned): note: exploit would have required a local login on mGuard
- Informational: GNU-wget vulnerabilities do not apply to mGuard as BusyBox-wget is used

1.2.23 Changes made between 2.1.1 and 2.1.2

- Corrected the Anti-Virus settings in the Factory Default profile
- Include log files into the support snapshot
- Fixed problem with the NTP service in stealth mode
- Fixed issue with logging of invalid packets in stealth mode

1.2.24 Changes made between 2.1.0 and 2.1.1

- Fixed problem with virus protection in PPPoE and PPTP modes

1.2.25 Changes made between 2.0.2 and 2.1.0

- Added virus protection functionality
- DHCP server supports static leases
- Voucher handling and new interim certification authority for licenses
- Integration with ISCM including firmware upgrade through configuration manager

1.2.26 Changes made between 2.0.1 and 2.0.2

- Fixed possible crash (reboot) in PPPoE mode
- Fixed possible hang in router mode
- Fixed failure to access device after switching to PPTP (static) mode
- Fixed possible failure of VPN reconnection with dynamic FQDN and PSK
- Applied security related patch for CAN-2004-0415
- Applied IXP400 Software patch for issue SCR32632
- Applied IXP400 Software patch for issue 081604

1.2.27 Changes made between 2.0.0 and 2.0.1

- Fixed problems in the update procedure from 1.1.x to 2.0.0
- Fixed incorrect permissions of the flash device files
- Fixed problems in handling the new “mGuard Enterprise” license

1.2.28 Changes made between 1.1.2 and 2.0.0

- Renamed “mGuard Gateway” product to “mGuard Enterprise”
- Fixed recently discovered security vulnerabilities in the Linux 2.4 kernel
- Added VPN tunnel connections in stealth mode
- Added configurable firewall rule sets to VPN tunnels
- Added SNMP management facilities (mGuard Enterprise)
- Added support for remote system logging (mGuard Enterprise)
- Added configuration profile save/restore functions
- Added NTP support
- Added firewall logging support
- Added support for DynDNS.org and DNS4BIZ dynamic DNS providers
- Added PPTP support for DSL providers
- Added Dead Peer Detection (DPD) for VPN
- Fixed issue “VPN reconfiguration in Stealth Mode”

1.2.29 Changes made between 1.1.1 and 1.1.2

- Fixed two recently discovered security vulnerabilities in the Linux 2.4 kernel
- Fixed security leak in anti-spoofing functionality
- Adapted bootstrap procedure and bootloader to changes in production environment
- Set re-keying retries for VPN tunnels to unlimited
- Fix possible alignment error in Frees/Wan (affected establishing VPN tunnels in special scenarios)

1.2.30 Changes made between 1.1.0 and 1.1.1

- Added L2TP support for router and PPPoE modes (Gateway and Core editions only)
- Added DES (56bit) support
- Added AES hardware acceleration support
- Added license management: number of VPN tunnels and L2TP support limited
- Fixed issue „AES software encryption only supports 128bit“

1.2.31 Changes made between 1.0.0 and 1.1.0

- Added DHCP server support for router and PPPoE modes
- Added DHCP client support for router mode
- Added DNS caching support for router and PPPoE modes
- Added dynamic DNS support
- Added CHAP support for PPPoE
- Added optional user authentication
- Added password protection for administrative access
- Added administrative access (HTTPS and SSH) from remote
- Added AES support for software encryption

- Fixed Issue „Port forwarding for ports 22 and 443”

1.2.32 Changes made between 0.8.5 and 1.0.0

- Added NAT-T support
- Fixed Issue „Busy Hub“
- Fixed Issue „Using certificates larger than 512Bytes in Stealth Mode“
- Fixed Issue „Port Forwarding“
- Fixed Issue „PSK in Stealth Mode“
- Fixed Issue „%any in Stealth Mode“ (see explanation in user manual)
- Fixed Issue „Connection startup in Stealth Mode“ (see explanation in user manual)

1.3 Updating from previous releases

Updating to 4.2.3 is supported from any 3.1.x, 4.0.x, 4.1.x and 4.2.x release. Devices still operating with older software versions must either be updated to 3.1.x first or may be installed from scratch using the flash mechanism. Please refer to the User Manual and the information coming with the update file for details.

- The “update-3.1.x-4.2.3” allows to update directly from all 3.1.x versions to 4.2.3.
- The “update-4.0.x-4.2.3” allows to update directly from all 4.0.x versions to 4.2.3.
- The “update-4.1.x-4.2.3” allows to update directly from 4.1.0 and 4.1.1 to 4.2.3.
- The “update-4.2.x-4.2.3” allows to update directly from 4.2.0, 4.2.1 and 4.2.2 to 4.2.3.

Starting with version 4.0.0 the “Automatic Update” feature may be used.

- From 4.0.x and from 4.1.x the 4.2.3 release is automatically chosen when using the “Install latest version” function.
- From 4.2.0, 4.2.1 and 4.2.2 the 4.2.3 release is automatically chosen when using the “Install latest patches” function.

1.3.1 Important update information (updating from 4.1.x, 4.2.0, 4.2.1 and 4.2.2)

- The update to the 4.2.3 release requires a reboot at the end of the installation. It is recommended to reboot as soon as the update procedure is finished and before making changes to the configuration.
- During update to the 4.2.3 release, the Anti-Virus scanner will be stopped and the Anti-Virus database is moved to a temporary location.
 - Connections normally protected by the Anti-Virus scanner will be blocked while the firmware update is in progress, such that no virus infected content can pass by.
 - In rare occasions it is possible, that the Anti-Virus database needs to be erased for the update to pass without errors. The device will then download the database anew after the update and reboot, as long as the update schedule is not set to “Never”.
- During update to the 4.2.3 release VPN tunnels may be stopped and restarted.
- During update to the 4.2.3 release informational messages about illegal values of configuration variables like “info: illegal value for 'VPN_DYNIP_SERVER' ignored” may be printed and logged. These can be ignored safely.
- During interactive update from 4.1.x to 4.2.3 release a message window is

displayed reading “Ignored changes on the previous page as it was not completely loaded.” The message can safely be ignored here (and only here).

1.3.2 Important update information (updating from 4.0.x)

- Versions 4.0.0 and 4.0.1 may lose VPN connections during update if more than half of the licensed number of tunnels is configured. Please save the configuration profile before updating so that the tunnels can be restored after the update.
- The update to the 4.2.3 release requires a reboot at the end of the installation. It is recommended to reboot as soon as the update procedure is finished and before making changes to the configuration.
- During update to the 4.2.3 release, the Anti-Virus scanner will be stopped and the Anti-Virus database is moved to a temporary location.
 - Connections normally protected by the Anti-Virus scanner will be blocked while the firmware update is in progress, such that no virus infected content can pass by.
 - In rare occasions it is possible, that the Anti-Virus database needs to be erased for the update to pass without errors. The device will then download the database anew after the update and reboot, as long as the update schedule is not set to “Never”.
- During update to the 4.2.3 release VPN tunnels may be stopped and restarted.
- During update to the 4.2.3 release informational messages about illegal values of configuration variables like “info: illegal value for 'VPN_DYNIP_SERVER' ignored” may be printed and logged. These can be ignored safely.
- During interactive update to the 4.2.3 release a message window is displayed reading “Ignored changes on the previous page as it was not completely loaded.” The message can safely be ignored here (and only here).

1.3.3 Important update information (updating from 3.1.x)

- The update to the 4.2.3 release requires a reboot at the end of the installation. It is recommended to reboot as soon as the update procedure is finished and before making changes to the configuration.
- During update to the 4.2.3 release the GUI and the authentication method will be changed.
 - At some point during the update your GUI connection to the mGuard will be stopped.
 - Please reconnect to the mGuard using your browser and login again using the new login window.
- During update to the 4.2.3 release VPN tunnels may be stopped and restarted.
- During update to the 4.2.3 release informational messages about illegal values of configuration variables like “info: illegal value for 'VPN_DYNIP_SERVER' ignored” may be printed and logged. These can be ignored safely.
- During interactive update to the 4.2.3 release a message window is displayed reading “Ignored changes on the previous page as it was not completely loaded.” The message can safely be ignored here (and only here).
- When using the 'upload' mechanism to install the update in rare cases no information about the progress of the update will be shown but the information page will be displayed immediately. The update will be performed nevertheless in

- the background. Information can be found in the system logfiles.
- When using the online update mechanism in rare cases error messages reading 'unable to change directory' are printed repeatedly. These can be ignored. The update will be performed nevertheless correctly.
 - During update to the 4.2.3 release, the Anti-Virus scanner will be stopped.
 - Connections normally protected by the Anti-Virus scanner will be blocked in this time, such that no virus infected content can pass by.
 - The previous scan engine is replaced by a new ClamAV engine. The AVP download URI is changed to the new address
downloads.avp.innominate.com
 - For the ClamAV engine only HTTP is supported as download protocol.
 - If AV is enabled, the scan engine will automatically start to download the latest AV pattern database after the reboot as long as the update schedule is not set to "Never".
 - *Please make sure that your AV license is still valid or disable AV services because new databases will not be loaded if the license is expired!*

1.3.4 Obtaining the update files

As of release 3.0.0 customers must register before downloading the update files for offline download or to access the online update server. Please refer to

http://www.innominate.com/register_software

http://www.innominate.de/register_software.

After registration user and password information is sent. Please note, that the update server is operating using the "https" protocol.

2 Identified Issues and Workarounds

Issue “mGuard MIB Replacement”

	Description
Synopsis	MGUARD-MIB has been replaced with MGUARDB-MIB
Symptom	Due to a restructuring of the SNMP service incompatible changes had to be made to the MIB. The MGUARD-MIB has therefore been replaced by the new MGUARDB-MIB which is using a new OID. mGuard releases up to 2.3.x must use the MGUARD-MIB, release 3.0.0 or later must use the new MGUARDB-MIB.
Workaround / action	Use the correct MIB for the release

Issue “Anti-Virus: operation on hardware with 32MB RAM”

	Description
Synopsis	Anti-Virus operation does not work on devices with 32MB RAM
Symptom	On devices with 32MB RAM only limited ramdisk space is available. Operation of AVP on 32MB devices is no longer supported.
Workaround / action	Contact your local dealer

Issue “Anti-Virus: update of local virus scanner”

	Description
Synopsis	Update of local virus scanner may fail with mGuard HTTP scan enabled
Symptom	The update/download of a virus scanner installed on one of the client PCs may fail, since the mGuard may detect virus patterns in the signature files and interrupts the download.
Workaround / action	Disable the HTTP-scanning (set Anti-Virus->HTTP-Options->Enable content scanning for HTTP to “No”) for the time of the download or apply a corresponding rule for the download/upload server to allow this traffic to pass unscanned.

Issue “Anti-Virus: active FTP in stealth mode with management IP”

	Description
Synopsis	In stealth mode with management IP the control connection is using the management IP of the mGuard while the data connection shall use the real IP of the client on the protected side. Some FTP servers (known: WU-FTPD) refuse to use different IP addresses for data and control connections with active FTP.
Symptom	The download/upload fails and the port command is rejected with '500 invalid PORT command' or a similar error (and a respective message may be logged on the FTP server).
Workaround / action	Use passive FTP instead.

Issue “Anti-Virus: multi stealth mode with logical subnetting”

	Description
Synopsis	In multi stealth mode the management IP is used by the mGuard to connect to (remote) locations. The Anti-Virus proxy uses this technique to open the connection to the requested server. If this server is located on the same physical network but a different logical network it is possible that the mGuard cannot reach the server from its management IP due to non-overlapping address ranges. In this case the Anti-Virus component fails.
Symptom	The connection attempt fails.
Workaround / action	Set up the list of servers to not include those on such logical subnets by adding the subnets with the “No Scan” option.

Issue “Anti-Virus: false virus detection”

	Description
Synopsis	Update or installation of software fails when loaded from network resources with false virus detection alarms
Symptom	A software or update package shall be installed from a network resource (for example the Internet). The download of the software fails and a virus detection is logged even though no virus is contained in the corresponding resource. This problem has been observed with binary packages for Windows and Linux operating systems. Note: some programs used to install software packages do not issue a suitable warning but just fail without proper diagnostics. Please check the Anti-Virus logs on the mGuard in this case. Note: this issue is equivalent to the issue "Anti-Virus: update of local virus scanner".
Workaround / action	Disable the HTTP-scanning (set Anti-Virus->HTTP-Options->Enable content scanning for HTTP to “No”) for the time of the download or apply a corresponding rule for the download/upload server to allow this traffic to pass unscanned.

Issue “AES hardware encryption only works with B0 stepping processors”

	Description
Synopsis	AES throughput is lower than for 3DES
Symptom	AES throughput values are lower than 3DES values. When checking the “System→Hardware→ CPU Stepping” information, an A0 stepping is shown.
Workaround / action	None. The A0 stepping of the Intel IXP4xx does not have the AES circuits built-in. The mGuard falls back to a software implementation. Only mGuards produced before November 2003 do have A0 stepping processors without AES hardware acceleration.

Issue “Static Stealth reconfiguration”

	Description
Synopsis	Changes are not correctly picked up in static Stealth Mode
Symptom	When changing the settings in static stealth mode, the changes are not honored after the OK button is pressed.
Workaround / action	Reboot the mGuard after making changes to the static Stealth configuration

Issue “MAU management not supported”

	Description
Synopsis	MAU properties cannot be set but a “not supported” message is shown instead.
Symptom	Earlier revisions of the PHY (physical access layer) chips used have a bug resulting in wrong value being seen when reading the registers. The problem has been fixed by the chip manufacturer in a later revision. This only applies to mGuard devices manufactured before Q3/2003. To prevent unexpected failures, only “auto negotiation” is supported on these devices.
Workaround / action	None.

Issue “AVP component: freeing connection slot”

	Description
Synopsis	The AVP (Anti Virus Protection) component does only allow a limited number of connections in parallel. Unused HTTP connections may be closed to improve mGuard resource usage.
Symptom	HTTP browsers (Internet Explorer, Opera, Netscape, ...) do open connections in parallel to download embedded information (images). For efficiency reasons these connections are kept open by the browsers (“keep alive” feature) to improve download speed for further pages from the same site. mGuard does only allow a limited number of concurrent virus scanned connections. If a new connection shall be opened and no connection slot is available anymore, mGuard will detect currently unused HTTP connections and close them in order to allow the new connection to succeed. Such event is logged as “freeing connection slot”.
Workaround / action	The ability to surf the Internet is not limited by the resource optimization handling. Most browsers allow to adjust the maximum number of concurrent connections a browser keeps open. The default settings typically will not lead to connection slot shortage.

Issue “H.323 Connection Tracking Disabled”

	Description
Synopsis	H.323 connection tracking support is disabled.
Symptom	Under rare conditions crashes of the system have been observed with H.323 connection tracking enabled and multimedia traffic. The connection tracking module has been disabled in the 3.0.0 release. Configuration options are still available for compatibility reasons but do not have any effect.
Workaround / action	None.

Issue “Pull Configuration Problems with Microsoft HTTP server”

	Description
Synopsis	Configuration pull fails with incomplete configurations being downloaded when the server is a Microsoft HTTP server.
Symptom	For some configurations with Win2000 (SP2 and SP4) incomplete transfers of configuration profiles using the “pull” method have been observed.
Workaround / action	Either update the operating system to Win2003 or install another HTTP server, for example Apache.

Issue “No Access To 1.1.1.1 With Management IP Address Set”

	Description
Synopsis	If a management IP address is set in stealth mode(s), access via 1.1.1.1 fails.
Symptom	Access via 1.1.1.1 is not supported in static stealth or multiple client stealth mode, if a management IP address is configured.
Workaround / action	Use the management IP address also from intern (protected port) to access the mGuard.

Issue “Power OK shown late on mGuard Blade”

	Description
Synopsis	The circuit checking the states of the redundant power supply units in the mGuard Blade does include filter capacitances. Due to these capacitances state changes are not signaled immediately. Power failure is signaled with a delay of 3-4 seconds, replacement of a power supply (now OK) is only signaled with a delay of 90 seconds.
Symptom	Display of the state of the power supply may still show failure even after the power supply has been re-enabled for 90s.
Workaround / action	None.

Issue “ICMP failure with transport VPN in Stealth Mode with SNMP”

	Description
Synopsis	ICMP echo requests are not answered through a transport mode VPN connection if the device is in Stealth Mode and SNMP is activated
Symptom	From a remote peer a client protected by an mGuard shall be pinged through a transport mode VPN. The tunnel is up and other traffic succeeds but ICMP echo requests are not answered. This problem only occurs if SNMP is enabled on the mGuard.
Workaround / action	None.

Issue “VPN firewall rule application for wrong tunnel”

	Description
Synopsis	If multiple tunnels are established to the same remote subnet originating from different local subnets, the firewall rules defined for the distinct tunnels are not handled correctly and interfere with each other. This interference only occurs between tunnels to the same remote subnet.
Symptom	Firewall rules intended to be used within one tunnel are applied to connections of another one.
Workaround / action	Use specific rules for the subnets used in the tunnel configuration instead of generic “0.0.0.0/0” type rules.

Issue “Administrative Access From Moved Client in Single Stealth”

	Description
Synopsis	In single stealth auto detect and static modes the client cannot access the mGuard if the client was moved to the extern (unprotected) side.
Symptom	In single stealth mode the mGuard records the client computer's IP and MAC address at the internal (protected) interface and uses it to direct traffic to the client. If the client computer is moved to the extern (unprotected) side and tries to communicate with the mGuard (even using the management IP address) communication is not possible, as the mGuard still tries to direct the traffic to the internal (protected) side.
Workaround / action	Do connect another client computer to the internal (protected) interface so that mGuard can learn new addresses for IP and MAC or reboot the mGuard.

Issue “ISCM: online firmware update can not be initiated”

	Description
Synopsis	An online firmware update can not be initiated through the Innominate Security Configuration Manager (ISCM) for devices already running a firmware version between 4.0.0 and 4.1.1 (inclusive).
Symptom	If a firmware update is initiated through ISCM the message window displays a message like “Update failed !!! update for device mguard1 failed! PEP Action terminated (failed).” The mGuard's firmware is not touched and remains in its previous stable state.
Workaround / action	Plan to update from firmware version 3.1.1 to 4.2.3 directly if possible. Otherwise use the mGuard's GUI to initiate the online update.

Issue “Traffic bypasses VPN during reconfiguration”

	Description
Synopsis	If a VPN connection is reconfigured (due to configuration changes) traffic may leave the mGuard unencrypted. This does not happen during firmware update. Firmware versions before 4.2.0 are affected unconditionally. Starting with firmware 4.2.0 it can happen under special conditions only: a) in stealth mode combined with transport mode connections and an open outgoing firewall (packet filter) and b) in stealth mode combined with tunnel mode connections, an open outgoing firewall (packet filter) and %any as the remote side it happens if the tunnel had been established and is taken down afterwards (for example by reconfiguration or restart of the peer).
Symptom	Traffic which is intended to be routed through a VPN connection occurs at the mGuard's external interface unencrypted and without VPN specific network translation applied.
Workaround / action	Add specific outgoing firewall rules to the main firewall configuration which drop or reject traffic to the remote networks which must be routed through a VPN connection only. Such rules will not match encrypted VPN traffic because VPN connections have separate firewall configurations.

3 Documentation Updates/Errata

- The mGuard delta is shipped without an RS232 serial cable though section 4.1 “Package contents” of the User's Guide lists it.
- Due to the fix of a security issue for ClamAV (CVE-2007-0897) the Anti-Virus scanner of the mGuard no longer scans MS Cabinet files though that file format is listed in chapter 1 of the User's Guide.